Information Services Board Briefing Paper on the Updated Statewide Information Technology Security Policy and Practices

Prepared by Mary Lou Griffith, DIS/MOSTD, (360) 902-2978.

Description

Digital government requires a secure and trustworthy environment for conducting sensitive transactions through open networks. To that end, the Information Services Board (ISB) initiated a comprehensive review and update of the statewide Information Technology (IT) Security Policy to address the security issues of conducting electronic commerce across the state enterprise. The IT Internet Security Program Charter was developed and approved at the June 12, 2001, ISB meeting. A recommendation that an Independent Security Analyst be assigned to report the status of the state's IT Security Program on a recurring basis was also approved by the Board at that time. Mr. Jeff Scheel was named as the ISB Independent Security Analyst and will report to the Board the current status of the IT Security program.

Background

Washington State government has been recognized as a leader in applying digital technologies and the Internet in service to the citizen. This has been achieved by leveraging the open architecture of the Internet to provide access to a wide range of public information and services.

Using the Internet to its greatest advantage requires a higher degree of security than was the case in an earlier era of closed systems and proprietary networks. Washington State government must take sufficient steps to ensure that citizens and businesses interacting with public agencies are protected by the appropriate information technology security. Beyond a range of anonymous exchanges available through the Internet, citizens and businesses need secure access to look up their medical or other benefit claims, exchange sensitive health records, and make or receive electronic payments with government. All these transactions require secure access control and data protection for the electronic exchange of information over the Internet. This is being done through the state's secure gateway, Transact Washington, which implements trustworthy access control through Public-Key Infrastructure (PKI).

Washington State government has set a clear direction and minimum standards for the way in which sensitive information and transactions are protected by state agencies. The policies, standards, and guidelines set the preconditions for achieving a consistent and reliable set of protections for sensitive information within a shared, trusted environment.

Status

The ISB Chair has responded to the letter from Governor Locke that directed certain actions to be taken to address security issues. The reply describes the policy development activities of the ISB and some of the initiatives underway to strengthen and increase the security of the state's infrastructure and the security awareness of state agency employees.

A security symposium was offered to agency business executives, information technology managers, and security managers on February 28, 2002 highlighting risks, threats, and vulnerabilities in the Internet realm. It provided information about the information technology security policy and the current security infrastructure. On March 1, 2002 sessions on the details of the security infrastructure were offered for technical staff.

Issues

- Some agencies addressed the potential impact of budget constraints on the development of comprehensive IT security program.
- Additional guidance may be needed on the development and implementation of effective Security Awareness Training.
- Many agencies identified significant work to be completed by June 30, 2002. The availability of adequate resources to complete the tasks was not addressed so the associated level of risk is difficult to discern.
- A draft charter was prepared and the Architecture Subcommittee of the Customer Advisory Board has been invited to participate and complete the charter for the establishment of the Washington Computer Incident Reporting Center (WACIRC).

Recommendation

DIS recommends that the Independent Security Analyst continue to report regularly to the Board on the status of the state's IT Security program and that the Board receive status of the agencies' security programs in the monthly update reports.